REMARKS:

In the outstanding Office Action, the Examiner rejected claims 1-17. Claims 1, 8 and 15-17 are amended herein. No new matter is presented. Support for the amendments can be found at least on page 7, line 21 through page 8, line 22.

Thus, claims 1-17 are pending and under consideration. The rejections are traversed below.

REQUEST FOR EXAMINER INTERVIEW:

Applicants respectfully request that the Examiner contact the undersigned at the Examiner's convenience, before acting on this case, to conduct an Interview to facilitate prosecution of the present application.

REJECTION UNDER 35 U.S.C. §103(a):

Claims 1-17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over various combinations of the following: Design of Conventional Cryptographic Algorithms reference by Preneel et al. (Preneel), U.S. Patent No. 6,501,840 (Saijo) and U.S. Patent No. 6,182,216 (Luyster).

Independent claim 1, by way of example, recites, "selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output number of the block", including determining "an optimal combination of input and output bit numbers of each of the S-boxes for usable memory capacity of said memory." Claim 1 further recites, "generating a plurality of S-boxes each having the input and output bit number selected by said selecting unit." Claims 8 and 15 recite similar features.

The claimed invention of claim 16 includes, "generating S-boxes each having an input and an output bit number selected based on memory capacity of a memory provided to the cipher device." Claim 16 recites that the input and output bit number is selected by "extracting a set of input and output numbers of the S-boxes as an optimal combination of input and output bit numbers based on an entire input and output bit number of a block and a minimum input and output number of the S-boxes."

Independent claim 17 recites, "determining an optimal input and output number of each of the S-boxes by generating a combination table having various sets of input and output

numbers of the S-boxes enclosable in a memory of the cipher device" and "selecting an optimal combination of input and output numbers of each of the S-boxes." Claim 17 further recites, "implementing the F-function by selecting said optimal combination of input and output numbers of the S-boxes from the combination table."

Preneel discusses proposals related to block ciphers, stream ciphers, and hash functions. Section 4.2 of Preneel discusses implementation of lookup tables or S-boxes including the DES that uses 8 different S-boxes with 6 input and 4 input bits and S-boxes with more output bits. Preneel merely mentions the concern that S-boxes should fit in the fast cache memory without describing how to implement S-boxes to fit the cache memory. In particular, Preneel does not teach or suggest the claimed "selecting" and "generating", as recited in the claimed invention (see discussion of claims above).

The Examiner acknowledges that Preneel does not disclose selecting an input and output bit number of the S-boxes each having the input and output bit number, but relies on Saijo as teaching the same. Saijo is directed to preventing a need to change a design of an apparatus when a new cryptographic processing type or a new algorithm type is devised (see, col. 2, lines 55-64). However, Saijo is limited to cryptographic processing that calculates the output data size according to the cryptographic processing type where a size of the input piece of the divided input data is equal to the data block size (see, col. 9, lines 17-36 and col. 10, lines 9-24).

The Examiner points out that Saijo discloses that "when the size of the input piece of the divided input data is equal to the data block size, the most efficient cryptographic processing is performed" at col. 9, lines 32-34. In contrast to Saijo's discussion that the most efficient cryptographic processing is performed when the size of the input piece of the input data is equal to the fixed data block size, the claimed invention enables use of the S-box having the largest size within the memory capacity of the primary cache memory, even when the largest size usable within the memory capacity is continuing to change while in operation.

In particular, the claimed invention generates S-boxes according to "an optimum combination of input and output bit numbers", thus not only can the high-speed accessible primary cache memory be fully utilized, but also the number of times for accessing the S-box can be reduced, thereby realizing high-speed cipher/decryption (see above discussion of independent claims and also Specification on page 7 line 21 to page 8 line 22).

Therefore, according to the claimed invention, the size of S-box is dynamically optimized, while Saijo is limited to dividing the input data by the fixed data block size of the memory.

Moreover, Saijo aims to divide the number of input data by the fixed and maximum size of memory. However, the claimed invention dynamically decides the numbers based on the size of usable memory in the cache memory.

On the other hand, Luyster encrypts a predetermined size input block and divides the input block into data segments using minimum size of round segments (see, col. 16, lines 59-64). However, the block size in Luyster is not variable and the minimum size of the round segments rotated by a data dependent variable is limited (see, col. 16, lines 63-65).

In light of the above, it is respectfully submitted that the independent claims are patentably distinguishable over the cited reference.

As dependent claims 2-7 and 9-14 depend from respective independent claims, the dependent claims are patentable over the references for at least the reasons presented above for the independent claims.

The dependent claims are also independently patentable. For example, claim 4 recites that the claimed invention, "tentatively decides an input and output number of each S-box by generating an input and output number of each S-box by dividing the entire input and output bit number of said block inputted from said input unit and allocating a remainder to the input and output number of an arbitrary S-box" and "combines the input and output numbers of the S-boxes tentatively decided within the memory capacity of said primary cache memory" (see also, claim 11).

The cited references, alone or in combination, do not teach or suggest the above-discussed features including "tentatively" deciding an input and output number of each S-box by "generating an input and output number of each S-box by dividing the entire input and output bit number of said block inputted from said input unit and allocating a remainder to the input and output number of an arbitrary S-box," as recited in claims 4 and 11.

Throughout the outstanding Office Action, the Examiner relies on well known and inherent basis for rejecting the claims. Specifically, the Examiner asserts that it is well known S-boxes are Feistel structure algorithms, padding a block at the end or remotest positions, size affects the efficiency and security of a cryptographic process and a minimum bound is required

to maintain satisfactory performance, and that it would be inherent to know the cache memory capacity to try to fit the S-boxes in the fast cache memory.

Applicants respectfully traverse the Examiner's statement because rationale or evidence tending to show inherency, and supporting evidence with respect to the well known rejection have not been provided, and request that the Examiner produce authority for the statement.

Further, Applicants specifically point out the following errors in the Examiner's well known rejection.

First, the Examiner uses common knowledge ("well-known") evidence for the rejection. As explained in the M.P.E.P.,

> any facts so noticed should... server only to "fill in the gaps" in an insubstantial manner which might exist in the evidentiary showing made by the Examiner to support a particular ground for rejection. It is never appropriate to rely solely on common knowledge in the art without evidentiary support in the record as the principal evidence upon which a rejection is based.

M.P.E.P. § 2144.03

Second, the noticed fact is not considered to be common knowledge or well-known in the art. In this case, the limitation is not of notorious character or capable of instant and unquestionable demonstration as being well-known. Instead, this limitation is unique to the present invention (see, M.P.E.P. § 2144.03(A) (the notice of facts beyond the record which may be taken by the Examiner must be "capable of such instant and unquestionable demonstration as to defy dispute").

Third, there is no evidence supporting the Examiner's assertion (see, M.P.E.P. § 2144.03(B) ("there must be some form of evidence in the record to support an assertion of common knowledge").

Fourth, the Examiner appears to be basing the rejections, at least in part, on personal knowledge. The Examiner is required under 37 C.F.R. § 1.104(d)(2) to support such assertion with an affidavit when called for by the Applicant. The Examiner is called upon to support such assertion.

Further, even if the Examiner's assertion and rejection based on common knowledge is valid, the claimed invention is distinguishable as discussed above.

Therefore, withdrawal of the rejection is respectfully requested.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 06/20/2007

By: Temnit Afework

Temnit Afework
Registration No. 58,202

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501